CITY OF SAN ANTONIO

Administrative Directive	**7.3a Data Security**
Procedural Guidelines	Regarding the use of public and confidential data
Department/Division	Information Technology Services Department (ITSD)
Revision Date(s)	September 13, 2019; September 6, 2021
Last Reviewed	November 1, 2022
Owner	Chief Security Officer

Purpose

This Administrative Directive ("AD") provides guidance for data governance as it relates to data security and compliance with federal and state related laws, regulations, and standards. This AD also establishes and identifies responsibility for data security and provides a framework for achieving compliance. Applicable security controls may include document marking/labeling, release procedures, privacy, transmission requirements, printing protection, computer display protections, storage requirements, destruction methods, physical security requirements, access controls, backup requirements, transport procedures, encryption requirements, and incident reporting procedures.

Documents related to this AD:

- COSA Data Governance AD 7.12
- Principles of Data-Informed Government
- AD 1.31 Open Records (Texas Public Information Act)
- AD 4.7 Healthcare Data Protection Administrative Authority
- AD 7.8D Access Control
- AD 7.4A Acceptable Use of Information Technology

Policy Applies To

☒ External & Internal Applicants	☒ Temporary Employees
☒ Full-Time Employees	☒ Volunteers
☒ Part-Time Employees	☒ Grant-Funded Employees
☒ Paid and Unpaid Interns	☒ Police and Fire Academy Trainees
☒ Uniformed Employees Under Collective Bargaining Agreements	

Definitions

Agency Sensitive Data	The data classification for data that has agency-specific value, the confidentiality and integrity of which must be protected to avoid adversely affecting the agency's interests. Agency Sensitive Data may be subject to disclosure or release under the Texas Public Information Act unless the information is otherwise defined as confidential by law or another exception under the Act applies.
Bring Your Own Device ("BYOD")	The practice of allowing the employees of an organization to use their own computers, smartphones, or other devices for work purposes.

City-administered information technology system(s)	Any technology or equipment that is used and/or managed by COSA even if COSA does not own the technology or equipment. COSA-managed information technology system(s) includes technology or equipment owned by COSA, on loan to COSA, funded by grants, or leased by COSA.
Confidential Data	Data that may not be freely released due to its protection by statute, regulation, or industry standards. Includes Sensitive Personally Identifiable Information.
Criminal Justice Information Services ("CJIS") Security Policy	CJIS Security Policy represents the shared responsibility between Federal Bureau of Investigation (FBI) CJIS and the CJIS Systems Agency and State Department of Public Safety.
Data Custodian	ITSD application and database owners who ensures that systems are properly maintained with good change-management procedures, so that data integrity is maintained and free from system corruption.
Data Owner	A Data Owner is the one who is responsible for the business relevance of the data generated in his/her organization, its operational value, its cleanliness, and overall data integrity. The Data Owner can also be a proxy owner if their org does not generate the data, but they are actually the authority that speaks to it in City of San Antonio.
Data Steward	COSA's Information Technology Services Department is the Data Steward responsible for data management and will establish appropriate governance and procedures required to ensure overall data integrity and reliability.
Network	A group of two or more computers linked together to facilitate communication, data sharing, and processing among other computer-based activities.
Personally Identifiable Information ("PII")	The data classification for information that alone or in conjunction with other information identifies an individual, including an individual's: (i) name, social security number, date of birth, or government-issued identification number; (ii) mother's maiden name; (iii) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image; (iv) unique electronic identification number, address, or routing code; and (v) telecommunication access device, including a card, plate, code, account number, personal identification number, electronic serial number, mobile identification number, or other telecommunications service, equipment, or instrument identifier or means of account access that alone or in conjunction with another telecommunication access device may be used to (a) obtain money, goods, services, or other thing of value; or (b) initiate a transfer of funds other than a transfer originated solely by paper instrument.
Record Retention Period	The minimum time that must pass after the creation, recording or receipt of a record or the fulfillment of certain actions associated with a record, before it is eligible for destruction pursuant to the Local Government Record Retention Schedules issued by the Texas State Library and Archives Commission under the authority of Subchapter J, Chapter 441 of the Texas Government Code.
Records Management Program	Established pursuant to Section 203.026 of the Texas Local Government Code and administered by COSA's Records Management Officer.
Sensitive Personally Identifiable Information ("SPII")	The data classification for Information that has not been made lawfully available to the public from the federal, state, or local government, including (i) an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:(a) social security number; (b) driver's license number or government-issued identification number; or (c) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; and (ii) information that identifies an individual and relates to: (a)

	the physical or mental health or condition of the individual; (b) the provision of health care to the individual; or (c) payment for the provision of health care to the individual.

Policy

Access to protected data shall be based on legitimate business need. COSA data shall be disseminated in accordance with this directive.

This directive applies to:

1. All data processed, stored, and/or transmitted by a COSA Information Technology System(s).
2. All COSA data processed, stored and/or transmitted on personally owned devices also referred to as Bring Your Own Device ("BYOD").
3. All data collected or maintained on a COSA owned and managed Network or authorized/contracted cloud platform by or on behalf of COSA in any form (electronic or hardcopy).

Adherence to this directive will help reasonably assure the confidentiality, integrity, and availability of COSA data:

1. COSA has adopted the National Institute of Standards and Technology ("NIST") Cyber Security Framework ("CSF") using 800-53A Security and Privacy Controls to provide a data protection framework for maintaining the confidentiality, integrity and availability of data.
2. Baseline security controls for COSA information systems shall be based on the Data Owner's data classification as governed by Data Governance AD 7.12.
3. The statutes and laws of the state of Texas and/or the state where the individual whose SPII was or is reasonably believed to have been acquired by an unauthorized person apply. Where statutes from another state conflict, the statutes of Texas and federal government shall take precedence.

Protection of Confidential Data

All departmental Data Owners must:

1. Implement cost effective internal controls, safeguards, and/or countermeasures to protect data. All preventative, detective, and/or corrective controls shall be risk based. The cost of all management, operational, and/or technical controls shall be commensurate with the value of the data.
2. Preserve citizen privacy and respect an individual's choice to consent when collecting, using, sharing, and/or disclosing of customer, partner, or employee personal information.
3. Limit the use and storage of confidential data and SPII to what is only necessary.
4. Not store confidential and/or sensitive data longer than is absolutely necessary past the established Record Retention Period.
5. Only collect data when COSA has the legal authority to do so and, if required, have a Privacy Act System of Records Notice ("SORN") in place that describes the information.
6. Minimize the distribution and proliferation of protected data.
7. Not store Agency Sensitive Data, Confidential Data, or business-related information in email, on personal devices, personal cloud storage, or any other non-COSA sanctioned storage.
8. Keep protected data relevant, accurate, timely, and not excessive in relation to the purpose such data is processed, stored, and/or transmitted.
9. Departments handling hardcopy or electronic Protected Health Information ("PHI") will

establish departmental procedures in accordance with AD 4.7 Healthcare Data Protection Administrative Authority for HIPAA.

The Data Custodian must:

1. Establish overall policies and procedures for dissemination of data in compliance with AD 1.31 (Open Records (Texas Public Information Act)), including establish and enforce departmental procedures that comply with this Directive and AD 1.31.
2. Determine encryption requirements based on regulatory requirements.
3. Periodically review data protection procedures, controls, and safeguards to reasonably assure that internal controls, countermeasures, and/or safeguards are working as intended. Ensure that at least once a year, COSA employees who have access to a COSA information system or database are identified and required those employees and COSA elected officials to complete a cyber security training program certified under Section 2054.519 of the Texas Government Code or offered under Section 2054.519(f) of the Texas Government Code. Requirement made by HB3834, takes effect September 1, 2019.Verify and report on the completion of a cybersecurity training program by required COSA employees.
4. Ensure that periodic audits are performed to ensure compliance with the cybersecurity training required by Section 2054.5191 of the Texas Government Code.

All COSA information systems must:

1. Use security controls to protect against unauthorized access, disclosure, modification, and destruction to reasonably assure the confidentiality, integrity, and availability of data.
2. Follow NIST encryption and security protocol standards for protected data as required.

Employee and third parties must:

1. Safeguard COSA's data resources and comply with the provisions of relevant COSA Security ADs.
2. Comply with all COSA procedures regarding protected data.
3. Receive written approval from his/her department Director to store sensitive data.
4. Report suspected violations to supervisor or manager, department head, and COSA Privacy Officer.
5. Only store protected data on COSA owned device(s) and/or device(s) managed by COSA even if COSA does not own the technology or equipment.
6. Ensure personal devices and personal accounts are not used to store, process, and/or transmit unencrypted protected data.
7. Not store Agency Sensitive Data, Confidential Data, or business-related information in email, on personal devices, personal cloud storage, or any other non-COSA sanctioned storage.
8. Ensure unencrypted confidential data and SPII is not transmitted outside of COSA.
9. At least once a year, if required, complete a cyber security training program selected by COSA.

Data Destruction

Electronic records shall be destroyed in accordance with Section 441.185 of the Texas Government Code and COSA Record Retention policies set out in AD 1.34 Records Management for Physical Electronic Records. All data storage device(s) and/or information system(s) containing protected data shall be sanitized or the storage device destroyed. COSA shall arrange for destruction of protected data by shredding, degaussing, erasing, and/or otherwise modifying the sensitive data in the records to make the information unreadable or indecipherable. Additional information on sanitization tools and methods of destruction based on Department of Defense 5220.22-M data destruction standards (available at http://www.dir.state.tx.us). Documentation shall also be maintained that documents the data, description

of device, data destruction process, and sanitization tools used to remove or destroy data.

Breach of Security of Computerized Data

In this section, "breach of system security" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by COSA, including data that is encrypted if the person accessing the data has the key required to decrypt the data.

1. **Report of Breach of System Security**
   Departmental Data Owners that discover a breach of system security must immediately contact COSA's Privacy Officer, the Director of the Information Technology Services Department, and the Administrator of the Office of the City Attorney.

2. **Notice to individuals whose sensitive personal information is disclosed in breach of system security**
   The Privacy Officer must notify individuals whose sensitive personal information is disclosed in a breach of system security without unreasonable delay and not later than the 60th day after the date on which COSA determines that the breach occurred; except that COSA may delay providing notice at the request of a law enforcement agency that determines that the notification will impede a criminal investigation.

3. **Notice to the Texas Attorney General**
   If the Privacy Officer is required to notify individuals of breach of system security and the breach involves at least 250 Texas residents, the Privacy Officer must also notify the Texas Attorney General of that breach not later than the 60th day after the date on which COSA determines that the breach occurred.

All breach of system security notices must comply with the notification requirements set out in Section 521.053 of the Texas Business and Commerce Code.

This directive supersedes all previous correspondence on this subject. Information and/or clarification may be obtained by contacting the Information Technology Services Department at 207-8888.

Roles & Responsibilities

Employees	Adhering to all guidance provided in this directive.
Departments	COSA departmental Data Owners are responsible for data classification and identification of data protection requirements in accordance with Data Governance AD 7.12.
ITSD	COSA Information Technology Services Department fulfills the role of the Data Steward and is responsible for publishing, disseminating, and maintaining this directive.